

# UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

TEXTNOW USER ACCOUNTS MMMYUMYUM11 AND  
MMMYUMYUM2

Case No. **1:23-MJ-00053**

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252	Certain Activities Relating to Material Involving the Sexual Exploitation of Minors
18 U.S.C. 2422	Coercion and Enticement

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jonathan P.R. Jones, SA FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
FaceTime Video Conference (specify reliable electronic means).

Date: **Jan 25, 2023**

City and state: Cincinnati, Ohio

*Stephanie K. Bowman*  
Judge's signature

Stephanie K. Bowman, United States Magistrate Judge  
Printed name and title



**Attachment A**

**Property to Be Searched**

This warrant applies to information associated with the TextNow accounts with username **“mmyumyum11” and “mmyumyum2” (TARGET ACCOUNTS)** that are stored at premises controlled by TextNow Inc., an electronic communications service provider headquarter at 420 Wes Graham Way, 2nd Floor, Waterloo Ontario, N2L 0J6 Canada, but with a United States presence at 1 Sutter Street, Suite 800 San Francisco, CA 94104.

**Attachment B**

**I. Information to be disclosed by TextNow**

To the extent that the information described in Attachment A is within the possession, custody, or control of TextNow, including any messages, records, files, logs, or information that have been deleted but are still available to TextNow, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), TextNow is required to disclose the following information to the government for each account listed in Attachment A:

- a. All contact and personal identifying information for the TextNow accounts with username **“mmyumyum11” and “mmyumyum2” (TARGET ACCOUNTS)** to include but not limited to full name, user identification number, date of birth, gender, contact e-mail, addresses, physical address (including city, state and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- b. All activity logs for the TARGET ACCOUNTS;
- c. All content of text messages sent and received;
- d. All photos and videos uploaded by the TARGET ACCOUNTS and all photos and videos uploaded by any users to the TARGET ACCOUNTS, to include metadata associated with those photos and videos;

e. All records or other information regarding the identification of the devices and internet browsers associated with, or used in connection with, the TARGET ACCOUNT, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

f. All information generated or received by the TARGET ACCOUNTS, including any postings, status updates, comments, networks or groups of which the user is a member, and information about the user's access and use of the TextNow application;

g. All other records and contents of communications and messages made or received by the users, including all public chat messages, private chat messages, group chat messages, chat history, video and voice calling history, and contact lists;

h. All IP logs, including all records of the IP addresses that logged into the TARGET ACCOUNTS;

i. All records of searches performed by the TARGET ACCOUNTS;

j. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

k. All records pertaining to communications between the TARGET ACCOUNTS and any other person regarding the ability to use and access TextNow, including contacts with TextNow support services and records of actions taken

- l. Any original metadata or file information still maintained by TextNow associated with media content sent to or from the user's TextNow account;
- m. Any cookies, web beacons, advertising IDs, and push tokens, associated with the TARGET ACCOUNTS; and
- n. The data listed above in paragraphs A through M shall be produced by TextNow regardless of where it may be stored.

**II. Information to be seized by the government**

- a. All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2422, including the following: All files, documents, communications, images, videos, contacts, metadata, and logs associated with the TARGET ACCOUNTS related to violation of Title 18 U.S.C. Section 2252 and Title 18 U.S.C. Section 2422, along with any evidence that would tend to show the true identities of the persons committing these offenses.
- b. All activity logs and IP logs, including all records of the IP addresses that logged into the account;
- c. Any communications in any format with Minor Victim A or relatives or friends of Minor Victim A;
- d. All account information, including:

e. All registration, identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

f. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

g. All privacy settings and other account settings;

h. All registered devices and accompanying serial numbers and other identifying numbers to include dates of activation, registration, deactivation;

i. All records pertaining to communications between TextNow and any person regarding the user or the user's TextNow account, including contacts with support services and records of actions taken;

j. All records that may identify co-conspirators, aiders, abettors, or any other individuals involved in the crime under investigation, including records that may help reveal their true identity and whereabouts; and

k. All records that may identify any victims of the crime under investigation;

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE  
SEARCH OF  
INFORMATION  
ASSOCIATED WITH  
TEXTNOW USER  
ACCOUNTS  
MMMYUMYUM11 AND  
MMMYUMYUM2

---

Case No. 1:23-MJ-00053

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH**

I, Jonathan P. R. Jones, depose and state under penalty of perjury as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with an account username of “mmyumyum11” and “mmyumyum2” (TARGET ACCOUNTS), that is stored at premises controlled by TextNow Inc., an electronic communications service provider headquarter at 420 Wes Graham Way, 2nd Floor, Waterloo Ontario, N2L 0J6 Canada, but with a United States presence at 1 Sutter Street, Suite 800 San Francisco, CA 94104. The information and accounts to be searched are also described in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation. I entered on duty as a special agent in 2007 and am currently assigned to the

violent crime squad of the Cincinnati Division. In this capacity, I investigate matters involving crimes against children, human trafficking, criminal enterprises, and other violent crimes. Prior to Cincinnati, I was assigned to the Toledo Resident Agency and the Lima Resident Agency of the Cleveland Division, where I was assigned a wide array of criminal and national security matters. During my tenure as a law enforcement officer, I have investigated a range of state and federal criminal violations, including those involving white-collar crime, violent crime, drug trafficking, crimes against children matters, and national security investigations. Since 2006, I have received training and have experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigation techniques, to include several Title III investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252, which criminalizes receipt, distribution, and/or possession of visual depictions of minors engaged in



sexually explicit conduct and Title 18, United States Code, Sections 2422, which criminalizes coercion and enticement of minors to engage in sexual activity, will be found in the **TARGET ACCOUNTS**. There is also probable cause to search the **TARGET ACCOUNTS** described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND ON TEXTNOW**

6. TextNow is a VOIP<sup>1</sup> service that allows users to text and call any number in Canada and the United States. TextNow provides the user with a real phone number to use and can be used on any smart device with an internet connection. The application can be used on multiple devices, including smartphones, tablets, laptops, or desktops. TextNow offers both free and paid accounts. Users in the United States can sign up for a free TextNow account

---

<sup>1</sup> VOIP (Voice over Internet Protocol), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

and can purchase a smart phone or a SIM card with a phone plan on TextNow's website.

7. TextNow assigns a ten-digit phone number identifier (three-digit area code plus seven-digit number) directly to the users once they have registered their account. TextNow users have the option to change their phone number every 15 days. TextNow recycles dormant phone numbers; therefore, a particular phone number identifier may be reassigned to different users at different times.

8. To access and use TextNow's services, a user must register and create an account. This can be done by either logging in with Facebook or by providing a username, email address, and password. TextNow asks users to provide basic contact information, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, and other personal identifiers.

9. TextNow collects different types of information about its users and their activities. TextNow collects information when a user registers, logs into, and uses TextNow, including the features used, the location of the user, and the information that a user enters and receives, such as chats and media files. TextNow has the ability to obtain and record information from a user's device or browser, including the IP address. Upon creation of the account, TextNow requests the user's location in order to assign a phone number in the user's area.

10. TextNow collects the content of text messages sent and received, and any media files that the user shared in the chat session, and a timestamp. Additionally, TextNow collects a record of all phone calls made from or received by a TextNow user, including the call start time and duration.

11. Therefore, the TextNow servers are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of TextNow, such as account access information, transaction information, and account application.

### **PROBABLE CAUSE**

#### **Kik Group Cincytaboo**

12. In August 2019, investigators assigned to the FBI Cincinnati Child Exploitation/ Human Trafficking Task Force were contacted by the Milford (Ohio) Police Department (MPD) and the Lockland (Ohio) Police Department (LPD) concerning a joint investigation in which William J Bustillos III (DOB XX/XX/1993) and Joseph L Suder (DOB XX/XX/1983) were both arrested and charged, in Hamilton County and Clermont County respectively, for the sexual assaults of three minors, in addition to state level charges of production and distribution of child pornography. During a law enforcement interview, Suder admitted to producing sexually explicit images of the two male minors, in addition to an eight year-female. Suder admitted to sexually assaulting all three minors. Suder admitted to sending the

sexually explicit images of the three minors to Bustillos. In return, Bustillos sent child pornography, of unknown minors, to Suder. Suder also admitted to trading images of the three minors in the Kik<sup>2</sup> application group called “Cincinnati Taboo”. Unknown persons in the group sent Suder child pornography, of unknown victims, in exchange for providing images of the three minors. Suder told investigators he deleted the Kik application from his cell phone prior to the interview. During his law enforcement interview, Bustillos admitted to exchanging child pornography with Suder. Bustillos admitted to participating in the production of child pornography of the three minors. Bustillos admitted to sexually assaulting the five-year-old male victim on numerous occasions, while Suder assaulted the other two children at the same time. Bustillos advised he used Kik and another application to send and receive child pornography. Bustillos also participated in the Kik group called “CincyTaboo”. Bustillos advised he deleted the Kik application from his cell phone just prior to his interview.

13. In February 2020, investigators with the Hamilton County Sheriff’s Office – Regional Electronic Crimes Investigation unit (RECI) conducted an investigation based on an Ohio Internet Crimes Against

---

<sup>2</sup> Kik Messenger, commonly called Kik, is a freeware instant messaging mobile application owned by holding company MediaLab.AI, Inc, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cell phone or other digital device.

Children Task Force lead. The investigation identified Ronald R Ledger Jr (DOB XX/XX/1977) as using the social media applications MeetMe and Kik to trade child pornography. During an interview, Ledger admitted to trading child pornography and to belonging to a Kik chat group called “Cincytaboo” in which child pornography was traded. Ledger provided investigators consent to search his cell phone and to assume control of his Kik account. RECI investigators captured the contents/communications from the Ledger’s Kik account. This included communications in the “Cincytaboo” chat group. The review identified “Cincytaboo” as being the group name, while the group hashtag was “#cincypervs”. Between approximately 02/26/2020 and 02/28/2020, RECI investigators monitored the communications in the “#cincypervs” chat group. On approximately 02/28/2020, Ledger’s account was removed from the group by the group administrator. Investigators were unable to rejoin the group after that date. The group chat had approximately 43 members as of 02/26/2020. Approximately 18 of the account profiles included both a display name and a username, while the remaining profiles only provided a display name. A review of the captured “#cincypervs” group communications indicated the person with a display name “BASTILLA Shan” and username “BASTILLA\_Shan” was an administrator in the group. The messages and images exchanged in the “#cincypervs” group included a message from username “BASTILLA\_Shan”, which stated “Friendly

reminder we have another group dedicated to young and only young stuff for those of u into it. Pm me. But will need new verification”

14. In responses to administrative subpoenas in March 2020, Kik provided subscriber information for the accounts that were members of the “#cincypervs” group. The response identified the account with username “BASTILLA\_Shan” was registered on 05/08/2019 with an unconfirmed email address of mmmymyum35@protonmail.com. An IP address of 98.28.219.33 was shown to have consistently been used to access the account between 01/03/2020 and 03/23/2020.

15. On 10/29/2020, Kik provided a search warrant return (USDC-SDOH Case No: 1:21-MJ-362) for the “BASTILLA\_Shan” account. The return contained 1,767 image and video files. A review of the files identified approximately 92 files which depicted prepubescent and post-pubescent males and females nude, partially nude, and/or engaged in sex acts, in which their genitals were depicted in lascivious manner.

16. On 10/22/2020, based on information obtained from Ledger’s access to the “Cincytahoo” Kik group and additional information for Kik account “Hayman5”, included in a June 2020 National Center for Missing and Exploited Children (NCMEC) Cyber Tip, a residential search warrant (USDC-SDOH Case No. 1:20-MJ-735) was executed at 3412 Mayfair Avenue, Cincinnati, OH. During an interview, Andrew Hay (born XX/XX/1996) was identified as the user of the “Hayman5” Kik account and Hay admitted to

having child pornography on his cell phone. Hay first obtained and viewed child pornography through the Kik application. Hay joined a Kik group called “Cincy Taboo” which had an administrator with a username of “Brastilla Chan”. Hay belonged to the group for approximately six months but was uncertain if the group was still active. When it was active, the group had up to 49 members at a time and members exchanged various types of pornography to include bestiality material and child pornography. Hay never direct messaged other members of the group. Hay posted homemade bestiality images/videos of himself engaged in sex acts with his own dog to the chat group. Hay estimated the youngest age of minors depicted in the images/videos sent in the group was seven-years-old. Hay advised that members of the “Cincy Taboo” Kik group directed him to start using the Telegram social media application<sup>3</sup>. The Telegram group communications contained child pornography. Hay identified the person with the Telegram username of Yum as the biggest provider of child pornography. Yum was also in the “Cincy Taboo” Kik group but Hay did not recall Yum’s Kik username.

---

<sup>3</sup> Per open source information, Telegram is a freeware, cross-platform, cloud-based instant messaging, video calling, and voice calling service. It was initially launched in 2013. The app servers of Telegram are distributed worldwide to decrease data load, while operational center is currently based in Dubai. The application is available for Android, iOS, Windows, macOS and Linux, operating system. Telegram provides end-to-end encrypted calls and optional end-to-end encrypted "secret" chats between two online users on smartphone clients, whereas cloud chats use clientserver/server-client encryption. Users can send text and voice messages, animated stickers, make voice and videocalls, and share an unlimited number of images, documents, user locations, contacts, and music.

17. A review was conducted of the content and communications on Hay's cell phone. It identified the Telegram messaging application as being installed on the device, with the account having a user name of "Haystack" and a user ID of 1029910772. Between 05/26/2020 and 09/27/2020, the account exchanged messages with a user name of "Yum" and a user ID of 733779667. The message exchanges included approximately 89 image and video files being sent. Most of the files were indicative of child pornography in that they depicted minors in various states of undress, depicted minors' genitals, and/or depicted the minors engaged in sex acts. In addition to the media files, text messages were exchanged. For instance, on 05/26/2020, the "Yum" user stated "Love watching pedos stroke off". Later in the exchange on that date, the "Yum" user asked "Got any lil boys" to which the "Haystack" user replied "I been having trouble finding little boys. I had some but had to delete them". On 05/28/2020, the "Yum" user advised he was near the "Kenwood Mall", to which the "Haystack" user replied he was from the Westside.

#### **NCMEC Cyberline Tips**

18. Between January 2020 and September 2021 social media platform providers submitted fifteen reports to NCMEC concerning suspected child pornography being associated with accounts in which the account user(s) uploaded the suspect material or otherwise accessed the accounts using the IP address 98.28.219.33. Below are summaries of the reports:



19. On 01/19/2020, Instagram<sup>4</sup> submitted a CyberTipline Report (63071247) regarding an account with the Telephone number: 646-305-5985, Email: ummheyhiitsthatcutekid@gmail.com, and Screen/User Name: “\_\_theonewhoknocks\_\_”, which was identified as uploading one file of suspected child pornography from IP address 98.28.219.33 on 01/18/2020.

20. On 01/25/2020, Instagram submitted a CyberTipline Report (63462178) regarding an account with the Name: Mia, Email: that1cutekidheyyy@gmail.com, Screen/User Name: “im\_ur\_qtpie”, which was identified as uploading one file of suspected child pornography from IP address 98.28.219.33 on 01/24/2020. Instagram provided images/videos in the report to NCMEC. A review of the images and videos appeared to depict two nude prepubescent females with their genitals exposed.

21. On 02/03/2020, Snapchat<sup>5</sup> submitted a CyberTipline Report (63984199) regarding an account with the Email: nowthatsyummy@protonmail.com, Username: “brakebillsalum”, which was identified as uploading one file of suspected child pornography from IP

---

<sup>4</sup> Instagram is social media application is social media application with a focus on sharing photos and videos. The application can be installed on cell phones and other internet connected digital media devices. The application allows that allows user to user text and multimedia instant messaging.

<sup>5</sup> Snapchat is social media application that allows user to user text and multimedia instant messaging, in addition to the posting of publicly viewable messages, images, and videos. The application can be installed on cell phones and other internet connected digital media devices. One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients. It also allows users to store photos in a password-protected area called "my eyes only".

address 98.28.219.33 on 01/30/2020. Snapchat provided an image in the report to NCMEC. A review of the image appeared to depict one nude prepubescent female with her genitals exposed.

22. On 02/07/2020, Kik submitted a CyberTipline Report (64176429) regarding an account with the Screen/User Name: “allurdreamz”, Email: mmmymyum69@protonmail, which was identified as uploading twenty suspected child pornography files between 01/19/2020 to 01/26/2020 from an IP address of 98.28.219.33. Kik provided images/videos in the report to NCMEC. A review of the images and videos appeared to depict nude prepubescent females and males with their genitals exposed and/or engaged in sex acts.

23. On 02/25/2020, Instagram submitted a CyberTipline Report (64934224) regarding an account with the Name: Mary Beth, Email: xuracheaterx@gmail.com, Screen/User Name: “aboutmarybeth”, which was identified as uploading two suspected child pornography files on 02/24/2020 from an IP address of 98.28.219.33. Instagram provided images in the report to NCMEC. A review of the images appeared to depict one nude prepubescent female with her genitals exposed.

24. On 03/15/2020, Snapchat submitted a CyberTipline Report (65966049) regarding an account with the Email: woopwoopdiwoop@gmail.com, Screen/User Name: “woopwoopdiwoop”, which was identified as uploading eight suspected child pornography files on

03/15/2020 from an IP address of 98.28.219.33. Snapchat provided images/videos in the report to NCMEC. A review of the images and videos appeared to depict nude prepubescent females with their genitals exposed and/or engaged in sex acts.

25. On 06/03/2020, Kik submitted a CyberTipline Report (73140787) regarding an account with the Email: mmmymyum101@protonmail.com, Screen/User Name: "ithelildevil", which was identified as uploading seven suspected child pornography files between 05/27/2020 and 05/30/2020 from an IP address of 98.28.219.33. Kik provided four videos and two images in the cyber tip to NCMEC. A review of the images and videos appeared to depict prepubescent females nude or partially nude in which the minors' genitals were depicted and/or the minors are engaged in sex acts.

26. On 06/29/2020, Snapchat submitted a CyberTipline Report (74269677) regarding an account with the Email: narglesnest@protonmail.com, Screen/User Name: "narglesnest", which was identified as uploading one suspected child pornography files on 06/25/2020 from an IP address of 98.28.219.33. Snapchat provided an image in the report to NCMEC. A review of the image appeared to depict one nude prepubescent female with her genitals exposed.

27. On 07/13/2020, Snapchat submitted a CyberTipline Report (74695224) regarding an account with the Email: narglesnest89@gmail.com, Screen/User Name: "anarglesnest", which was identified as uploading one

suspected child pornography files on 07/12/2020 from an IP address of 98.28.219.33. Snapchat provided an image in the report to NCMEC. A review of the image appeared to depict one nude prepubescent male with his genitals exposed.

28. On 08/25/2020, Snapchat submitted a CyberTipline Report (77716147) regarding an account with the Email: mmmyumyum66@gmail.com, Screen/User Name: “narglenest”, which was identified as uploading one suspected child pornography files on 08/25/2020 from an IP address of 98.28.219.33. Snapchat provided an image in the report to NCMEC. A review of the image appeared to depict one nude prepubescent female engaged in a sex act.

29. On 08/26/2020, Snapchat submitted a CyberTipline Report (77757459) regarding an account with the Email: mmmyumyum@protonmail.com, Screen/User Name: “ithinkimyummy”, which was identified as uploading two suspected child pornography files on 08/25/2020 from an IP address of 98.28.219.33. Snapchat provided an image in the report to NCMEC. A review of the image appeared to depict two nude prepubescent females with their genitals exposed and/or engaged in a sex act.

30. On 11/10/2020, Kik submitted a CyberTipline Report (82713310) regarding an account with the Email: mmmyumyum77@gmail.com, Screen/User Name: “hotterwhensmaller”, which was identified as uploading twenty-eight suspected child pornography files on 10/24/2020 from an IP

address of 98.28.219.33. Kik provided twenty-eight files to NCMEC. A review of the images and videos appeared to depict prepubescent males and females nude or partially nude in which the minors' genitals were depicted and/or the minors were engaged in sex acts.

31. On 09/23/2021, Instagram submitted a CyberTipline Report (102393525) regarding an account with the Phone: 646-305-5985, Email: ummheyhiitsthatcutekid@gmail.com, Screen/User Name: "\_\_theone\_\_1", which was identified as uploading two suspected child pornography files on 05/13/2020 from an IP address of 98.28.219.33.

32. On 09/23/2021, Instagram submitted a CyberTipline Report (102396110) regarding an account with the Email: itsmeitsjoc@gmail.com Screen/User Name: "ohimimim", which was identified as sending seven suspected child pornography files to three other users between 10/01/2019 and 04/06/2020. The "ohimimim" account was accessed from an IP address of 98.28.219.33 on 03/26/2020.

33. On 09/23/2021, Instagram submitted a CyberTipline Report (102400000) regarding an account with the Name: "\_\_1GAF\_\_щe1я\_\_Ass", Email: rudithezombrose@gmail.com, Screen/User Name: "\_\_least.im.a.real.bish\_\_", which was identified as sending thirteen suspected child pornography files to another user between 02/19/2020 and 02/20/2020. The receiving account was identified with a Name: "anon",

Phone: 646-305-5985<sup>6</sup>, Email: ummheyhiitsthatcutekid@gmail.com,

Screen/User Name: “\_\_theone\_\_1”. The “\_\_least.im.a.real.bish\_\_” account was accessed from an IP address of 98.28.219.33 on 03/07/2020.

34. Subpoena responses in May 2020 and January 2021 from Charter Communications identified the IP address 98.28.219.33 was assigned to a residence at 5504 E Galbraith Rd, Apt 12, Cincinnati, OH 45236-2839, from 01/03/2020 to at least 01/12/2021.

**5504 E Galbraith Rd, Apt 12, Cincinnati, OH**

35. In December 2020, employees with the Indian Creek Apartments confirmed Jocko Rosello (Born XX/XX/1989) and his mother resided at 5504 E Galbraith Rd, Apt 12, Cincinnati, OH 45236-2839. Criminal history checks indicated Rosello was arrested in 2016 and charged in Kentucky with a state violation of using an electronic communication system to procure a minor for sex. According to law enforcement reports, in July 2016 a law enforcement officer observed a Craigslist.com advertisement that was advertising "any girl into perv and taboo". The advertisement also advertised for a girl into incest, young, etc. An undercover law enforcement officer (UCO) responded to the advertisement under the guise of being a 14

---

<sup>6</sup> The is the same telephone number as the suspect accounts in the above referenced CyberTipline Reports 63071247 and 102393525.

year-old female. After exchanging emails, the UCO and Rosello switched to the Kik application. Rosello discussed wanting the UCO to send nude photographs and mentioned it would make him feel safer about coming to Louisville, Kentucky because he knew that law enforcement officers couldn't do that. Rosello also discussed viewing pornography, to include child pornography, with the UCO. Rosello also told the UCO he kept a collection of child pornography on a thumb drive. As of January 2023, there is no judicial adjudication in this case.

36. In January 2021, investigators executed a residential search warrant (USDC-SDOH Case No: 1:21-MJ-029) at 5504 East Galbraith Road, Apartment 12, Cincinnati, Ohio 45236. Rosello and his mother were located inside the residence. Both acknowledged living at the apartment. Rosello, was interviewed and several electronic devices were seized from the residence. Rosello denied any knowledge of the “BASTILLA\_Shan” and “ithelildevil” Kik accounts nor the “#cincypervs” Kik group chat. He denied being associated with child pornography. Rosello did acknowledge having a guitar in a case in his bedroom. He asserted a Samsung brand laptop computer, an Alcatel brand One Touch Tablet, a Motorola brand cell phone, and sex toys, located in the case with the guitar were old and had not been used in years. Rosello initially denied knowing the below referenced Minor Victim A. Rosello was shown images of an envelope and card from Minor Victim A, which included the hand-drawn depiction of two characters with

the names [Redacted-Minor Victim A first name] and Joc, that was located in his bedroom. The envelope was addressed to Jason at 5504 East Galbraith Road, Apt 12, Cincinnati Ohio. The return address had Minor Victim A's name and home address listed. Inside the envelope was a homemade bracelet and card with a poem written on it. Rosello responded that he had nothing to say about the card. Rosello denied communicating with the mother of Minor Victim A nor being aware of the significance of the user name "Averyconcernedfriend". At the end of the interview, Rosello acknowledged that the evidence showed it was him, but asserted it was a giant setup.

37. A review of the devices seized from Rosello's residence, indicated that Rosello used social media applications, such as Kik and Telegram, and possibly other unknown means, to send and receive child pornography. Numerous images and videos of minors nude and/or engaged in sex acts were located on the Alcatel tablet, the Motorola cell phone, and two hard drives recovered from Rosello's bedroom. A review of the Alcatel tablet, showed the device was logged into the Kik account iTheLilDevil<sup>7</sup> account, with an email mmmmyumyum101@protonmail.com, and showed child pornography was being traded with other Kik users.

38. A review of the Motorola cell phone located records for variations of the mmmmyumyum alias. Contacts for mmmmyumyum and a

---

<sup>7</sup> See above referenced February 2020 NCMEC Cyber Tipline Report.



mmmyumyum1@protonmail.com were located in the device's contacts application. Autofill records for mmmyumyum@protonmail.com and mmmyumyum15@protonmail.com were located. A reference to mmmyumyum@protonmail.com was found in the web history. A reference to a mmmyumyum2@gmail.com associated with the Grindr application. Additionally, a reference to "mmmyumyum2" was identified in a data file in a file subfolder named "TextNow".

39. A review of communications in Telegram application on the Motorola cell phone located the above referenced message exchange from the Telegram application on Andrew Hay's cell phone. Information from the Alcatel Tablet showed the Telegram application had a Username: "ThatsYummy" and Telephone: 646-305-5985<sup>8</sup>. The review of the Telegram application showed child pornography was being traded with other users in addition to Hay.

40. Information regarding Minor Victim A was located on both the Motorola cell phone and Alcatel Tablet. The Minor Victim A's first name and telephone number were located in the contacts of the tablet. The cell phone contained several references to Minor Victim A's first and last name, along with her email account, under the user accounts on the device. Minor Victim A's email and birthday were listed in the Calendar application. Emails were

---

<sup>8</sup> See above referenced CyberTipline Reports 63071247, 102393525, and 102400000.

located which showed exchanges between Minor Victim A's email account and an email account of zmeyaven1@gmail.com in March 2020 and email account thatonecutekidhi@gmail.com in April 2020. The Motorola cell phone also contained over forty non-explicit images/videos of Minor Victim A and screenshots/screen videos of her apparent Snapchat account.

41. The review of both the Motorola cell phone and the Alcatel tablet also located visually identical sets of five videos featuring Minor Victim A which appeared to have been saved on the cell phone on 12/16/2019 and on 12/19/2019 on the tablet. On both devices, the videos appeared to be saved in the Telegram application. Those videos are further described as:

- a. 1\_5170316652088131779.mp4 - a seven second video of Minor Victim A, from waist down, taking a selfie video, masturbating her vagina. She is wearing what appear to be red, white, and green pajamas with hearts and "Love" written on them, as well as a purple-colored, interwoven ring on her right index finger.
- b. 1\_5170316652088131780.mp4 - a fourteen second video of Minor Victim A, from waist down, taking a selfie video, masturbating her vagina. She is wearing the same type pajamas and the same purple ring as in the first video.
- c. 1\_5170316652088131781.mp4 – a six second selfie video showing Minor Victim A's face. She is licking her breast and has the same purple-colored interwoven ring on her right index finger.

d. 1\_5172766406944489604.mp4 - a two second selfie video of Minor Victim A. It does not show child pornography, but clearly shows her face. She is wearing a “Kings Island” shirt, stating unrecognizable sentence.

e. 1\_5177385300673953916.mp4 – an eleven second video, taken from the waist down. Minor Victim A exposes her vagina and masturbates with her right hand. She is wearing the same purple-colored interwoven ring on her right index finger.

42. On 01/27/2021, Rosello was arrested via complaint (USDC-SDOH 1:21-MJ-00069) and indicted in March 2021 (USDC-SDOH 1:21-CR-007) on one count of Receipt and one count of possession of child pornography (18 USC § 2252A).

### **Minor Victim A**

43. In September 2020, investigators were contacted by the parents of Minor Victim A, date of birth XX/XX/2003, regarding telecommunications harassment. Minor Victim A met the subject, “Jack”, online in late 2019. They chatted mostly through Instagram, although Minor Victim A could not remember Jack’s Instagram screen name. Minor Victim A stated that she sent Jack two images of herself exposing her breasts and vagina. Minor Victim A began receiving messages from numerous unknown phone numbers and screen names, threatening Minor Victim A and her family. The subject

told her that if she did not break up with her boyfriend, he would send the images she sent, to her school. Once she did this, he stopped contacting her for some time.

44. The subject began contacting Minor Victim A again, threatening her and her family. He told her that if she sent him a naked image of herself, he would stop. Once she sent the image, though, the messages continued and she became more fearful of what he would do, especially to her family.

45. The subject also sent her a Wyze wireless internet camera and told her to put it in her bedroom so he could “make sure she was doing what she was supposed to.” Not long after she set up the camera, two Instagram accounts appeared and began following people in Minor Victim A’s family. One was Venk836228, which was a variation of Minor Victim A’s name. The other, Averyconcernedfriend1, was similar to one of the email addresses that sent her messages. That email account, aconcernedfriend1@protonmail.com, also began emailing Minor Victim A’s mother on her personal and work account.

46. In January 2021, investigators sent a subpoena to Instagram, requesting subscriber information for the accounts, Venk836228 and Averyconcernedfriend1. Instagram’s response identified the Averyconcernedfriend1 account was registered on 09/12/2020 with an email address of aconcernedfriend1@protonmail.com from an IP address of 98.28.219.33.

47. Pursuant to consent, investigators conducted a forensic extraction of Minor Victim A's cell phone. A review of the extracted data located three 09/11/2020 voicemails in which a male, whose voice appeared consistent with Rosello's, apologized to Minor Victim A., advised that he loved her, and for her to let him know that she was alright. An undated image of Rosello was also located.

48. The forensic extraction of Minor Victim A's cell phone also located approximately 345 messages exchanged with telephone number 513-880-6573 on 09/11/2020. The extraction included texts but did not appear to include any associated image/video files which may have been sent in the exchange with 513-880-6573. At the beginning of the exchange, it appears Minor Victim A and the user of 513-880-6573 are connected via audio or video. Minor Victim A further indicated the user of 513-880-6573 had access to Minor Victim A's Snapchat account. The exchange then turned into disagreement about when the user of 513-880-6573 allegedly asked Minor Victim A to have sex with his cousins. Minor Victim A told a third-party about the request. The user of 513-880-6573 then threatened to assault or even kill the third party for knowing this information. Minor Victim A repeatedly asked that the third-party not be hurt. The following exchange then occurred:

From	To	Direction	Message
+15138806573		Incoming	I'm sorry. I cant risk my family. If it was ur brothers u would wanna do same thing
	+15138806573	Outgoing	No I wouldn't have
	+15138806573	Outgoing	Bc I wouldn't have asked someone to fuck them
	+15138806573	Outgoing	Tf
+15138806573		Incoming	I didnt ask u to fuck them? We were talking about if u liked that. And I said well.if u do I could let u with my cousins. I never once said i WANT u to do that. I said if ur into it u can. Ur acting like that was a conversation where I was being a dick or forcing u and it wasnt. We were having a good talk that day
+15138806573		Incoming	Then u went and told this dude that I tried to force u to
+15138806573		Incoming	The only thing I've ever forced u to do is stop talking to people. I've never forced u to do shit else. Even the nude thing the fee times we did it I didnt say do this or I hurt u.
	+15138806573	Outgoing	I never told him u forced me
	+15138806573	Outgoing	And u implied that u wanted it
+15138806573		Incoming	He specifically said the word force
+15138806573		Incoming	He even asked if I had "forced you to be with anyone else"
+15138806573		Incoming	And no I didnt. The conversation wasnt even about my cousins it was about the other thing and u saying u thought u like it

			but didnt kno. And thays when I offered u the chance so u could try and see
+15138806573		Incoming	And lol ofc I'd wanna see that tho who wouldn't
	+15138806573	Outgoing	Well maybe he misunderstood
+15138806573		Incoming	Can we talk about something else. I dont wanna argue with u. I just wanna be cool
+15138806573		Incoming	And can u angle the cam down, that way we never have to argue about what.ur doing anymore. I wanna try cut out all our problems and issues that start fights

49. After some additional exchanges, the user of 513-880-6573 advised “I'm going to overnight a new camera to you that looks like a charger or clock”. To which Minor Victim A responded ok, then they appear to confirm the house number of Minor Victim A’s residence. The following exchange then occurred:

From	To	Direction	Message
+15138806573		Incoming	Go on amazon or something and look at the cameras and pick on u can make work
+15138806573		Incoming	Can try Walmart too
	+15138806573	Outgoing	Ok idc
+15138806573		Incoming	Well just look thru both and pick one u can use
	+15138806573	Outgoing	Ok

+15138806573		Incoming	Ur gonna get busted using that book. So we gotta swap it up
	+15138806573	Outgoing	Okay hold on I'm doing laundry
+15138806573		Incoming	What time do you wanna try the jailbreak
	+15138806573	Outgoing	Idk
+15138806573		Incoming	Ok...
	+15138806573		[No Content In Extraction Report]
+15138806573		Incoming	Well we need to
	+15138806573	Outgoing	I know
	+15138806573		[No Content In Extraction Report]
+15138806573		Incoming	I'll look into it. Has to be able to be plugged in and stuff too
	+15138806573	Outgoing	Ok
+15138806573		Incoming	Can I ask a dirty question
	+15138806573	Outgoing	What
+15138806573		Incoming	Would u put that pen inside urself with the camera on so we could see what it looked like lol
	+15138806573	Outgoing	Would that get u money
+15138806573		Incoming	No lol just something interesting ive never seen
	+15138806573	Outgoing	Ok
+15138806573		Incoming	Let's go to snap I think my texts are delayed here



50. After more exchanges, the user of 513-880-6573 questioned the current location of Minor Victim A, saying Minor Victim A was not at work like she said. The user of 513-880-6573 then sent consecutive messages stating: “Well hope ur happy. Might ad well kill urself”, “I called ur job.... idk why ur acting”, “Fuck u then I'm calling cops on us both”, and “Answer I'm 3 way calling the cops”. Shortly after those messages, the following exchange occurred:

From	To	Direction	Message
+15138806573		Incoming	There is 0 chances from here on. We are totally done
+15138806573		Incoming	Hope it was worth it
+15138806573		Incoming	Get nice and high and suck that dick real good
	+15138806573	Outgoing	I ain't sucking no fucking dick
	+15138806573	Outgoing	Why'd you fucking send that
+15138806573		Incoming	Because ur a liar and im.done
+15138806573		Incoming	I'm not joking here
+15138806573		Incoming	The bad ahit is going as soon as I edit out the illegal parts
+15138806573		Incoming	If u think I'm giving u another chance and not actually gonna send this shit u are sadly mistake.
+15138806573		Incoming	I begged u and begged u

+15138806573		Incoming	I begged u and begged u
+15138806573		Incoming	And that entire convo was just a lie
	+15138806573	Outgoing	Why the fuck did you do that
	+15138806573	Outgoing	They're picking me up
	+15138806573	Outgoing	Fuck
+15138806573		Incoming	There's alot more coming

51. Following the exchange, Minor Victim A advised she was with her parents, and they were taking her phone. The user of 513-880-6573 threatened to message Minor Victim A's father and then he was sending something to the brothers of Minor Victim A's friend. The last message from Minor Victim A was a statement to stop texting her, to which the user of 513-880-6573 replied no.

52. Screenshots of the above referenced message exchange were also obtained from the forensic extraction. The screenshots included many of the above cited messages, but also included additional messages not recovered from the Chat portion of the forensic extraction. In one screenshot, the user of 513-880-6573 appears to send a message of a Snapchat profile in which Minor Victim A's breasts are depicted. In another message, the user of 513-880-6573 identified himself as twenty-three year-old Tyler Johnson.

53. In another series of screenshots, after Minor Victim A called the user of 513-880-6573 a stalker, the following exchange occurred:

From	To	Direction	Body
	+15138806573	Outgoing	You're completely dismissing what I'm saying
+15138806573		Incoming	Ur saying I'm a stalker... I said ok maybe I fit the definition. But doesnt change why I'm doing it or the situation we are in
	+15138806573	Outgoing	"I fit the definition" lol doesn't fucking matter why ur doing it the fact that you're doing it and have been doing it for so long is fucked up
	+15138806573	Outgoing	And the fact you don't see whats wrong with that is even more fucked up
+15138806573		Incoming	Yea I agree. And the fact that I've had to because u csnt keep ur pussy in ur pants is fucked too
+15138806573		Incoming	Oh believe me I know
	+15138806573	Outgoing	Then don't fucking do it
+15138806573		Incoming	Why do you think I'm willing to go to jail
	+15138806573	Outgoing	Being sexually active is a lot different than stalking

54. In another screenshot, Minor Victim A messaged “ What’s destructive is you fucking stalking and extorting me”, to which the user of 513-880-6573 replied “I sat here and promised I’d leave u alone if the therapy and being good didn’t make u feel better in a few weeks”, “But u just wanna sext guys idk”.

55. Another screenshot contained the following exchange:

From	To	Direction	Body
+15138806573		Incoming	I hate u for making me ruin ur life
	+15138806573	Outgoing	Me? How am I making you do this
+15138806573		Incoming	Because we agreed to everything and now u backed out
+15138806573		Incoming	I said camera.until we jailbreak and root and u said deal
+15138806573		Incoming	But doesn’t Matter I just did the first step
	+15138806573	Outgoing	Because I realized my own worth
	+15138806573	Outgoing	And it's more than being fucking stalked

+15138806573		Incoming	Ok well give it about 5 minutes
	+15138806573	Outgoing	Wdym
+15138806573		Incoming	You'll see
+15138806573		Incoming	Just to show u I ain't bluffing
	+15138806573	Outgoing	Don't fucking do this please

56. In addition to the text message screenshots, additional pertinent screenshots were recovered from Minor Victim A's cell phone. This included images of an apparent Instagram social media application with Instagram user “\_\_theonewhoknocks\_\_”<sup>9</sup> and images of Snapchat chat exchanges with one account with a user name of “newmesameyou” and a display name “Its Me” and another Snapchat account with a display name of “Joc”. In the exchange with “Its Me”, the user threatened to expose all of Minor Victim A's alleged activities to her parents, to include videos and screenshots of her sexting and cheating.

57. In January 2023, pursuant to a subpoena, Snapchat Inc provided records for the account with a username of “newmesameyou”. The records identified the account as being created on 03/15/2020 from an IP address of 98.28.219.33. The user provided an email address of [mmmyumyum1@gmail.com](mailto:mmmyumyum1@gmail.com). The user provided a display name of “Its Me” at the time of account creation. The account user changed the password on 01/25/2021.

---

<sup>9</sup> See above referenced January 2020 NCMEC Cyberline tip from Instagram.

58. On 01/26/2021, a follow-up interview of Minor Victim A was conducted after the initial review of Minor Victim A's cell phone and preliminary review of the Alcatel tablet recovered from Rosello's residence. Minor Victim A advised she chatted with a person she believed was a 22 year old man named "Tyler" on Snapchat. "Tyler's" username was "It's Me". During their chats, he coerced her into sending several naked images and videos to him. He also sent her a Wyze internet camera and told her to set it up in her room. If she did not have the camera on he would threaten her by saying he would send the videos and images out to her friends and school.

59. At the same time she was chatting with "Tyler", she was also chatting with "Joc" on Snapchat. Minor Victim A met "Joc" on Instagram in March of 2020. He told her he was 22 years old and lived in Kenwood, Ohio. During their chats, she told him about "Tyler" and how he was threatening her. "Joc" told her that he would help her and said he hired a private detective to try to find "Tyler's" internet protocol address to determine his real identity and where he lived. At some point during their chats, Minor Victim A told "Joc" she was 16 years old and in high school. "Joc" wanted to meet with Minor Victim A, but she stated she never met him.

60. Investigators showed Minor Victim A the image of Rosello recovered from her cell phone. When asked her if she recognized him and how. Minor Victim A stated that the picture was of the man she knew as "Joc". She was also asked if she ever mailed him anything. She said she had

made him a bracelet and a card and mailed it to his address on Galbraith Road. He told her to address it to "Jason". Investigators showed Minor Victim A images of the envelope, bracelet and card, that was recovered from Rosello's residence. She identified it as the package she mailed to him.

61. Investigators showed Minor Victim A sanitized screenshots of the above referenced five videos located on the Motorola cell phone and Alcatel tablet. She positively identified herself in each one and stated that they were taken in her bedroom. She stated that she sent more videos than the five that were recovered.

62. In response to a subpoena in December 2022, TextNow provided records for telephone number 513-880-6573. Telephone number 513-880-6573 was assigned to an account with a username: mmmymyum11, with an email mmmymyum11@protonmail.com, from 09/07/2020 14:02:00 UTC to 09/14/2020 22:42:45 UTC with a registration IP address of 98.28.219.33. The TextNow records indicated 1226 text messages were exchanged with the Minor Victim's telephone number between 09/07/2020 and 09/11/2020. The TextNow records also appeared to indicate the text messages were not deleted and may still be on the TextNow server.

63. In response to a subpoena in January 2023, TextNow provided records for accounts mmmymyum11 and mmmymyum2. The records identified that in addition to the 513-880-6573 telephone number, the mmmymyum11 account was also assigned telephone number 513-912-8287

from 09/14/2020 22:43:31 UTC to 10/16/2020 05:52:29 UTC. The records identified the mmmyumyum2 account as being registered on 08/09/2019 from a IP address of 74.83.138.114<sup>10</sup>, with an email of mmmyumyum2@protonmail.com. Five telephone numbers were assigned to the mmmyumyum2 account between January 2020 and November 2020. The telephone numbers and date ranges are as follows.:

269-367-7363 from 01/01/2020 05:00:00 UTC to 02/08/2020 11:41:33 UTC

269-479-4346 from 02/11/2020 14:48:06 UTC to 02/20/2020 11:40:59 UTC

937-764-4476 from 02/28/2020 18:17:08 UTC to 10/12/2020 04:44:44 UTC

937-606-8329 from 10/12/2020 14:30:48 UTC to 10/20/2020 04:46:36 UTC

513-880-9096 from 11/04/2020 23:41:05 UTC to 11/12/2020 04:52:29 UTC

64. Records provided by Kik in April 2021, identified the above referenced “bastille\_shan” account as being accessed from IP address 74.83.138.114 from 08/23/2019 to 09/22/2019. A December 2021 subpoena response from Google Inc, identified email address itsmeitsjoc@gmail.com<sup>11</sup> as being registered on 09/17/2019 from IP address 74.83.138.114. A related September 2021 subpoena return from Instagram identified the account

---

<sup>10</sup> This IP address was assigned to Cincinnati Bell, however, the usage dates were beyond Cincinnati Bell’s IP assignment retention records.

<sup>11</sup> See above referenced CyberTipline Report (102396110) from Instagram in September 2021.

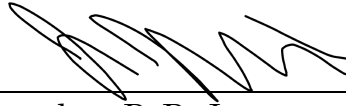
associated with the [itsmeitsjoc@gmail.com](mailto:itsmeitsjoc@gmail.com) email as also being accessed from IP address 74.83.138.114 on 09/17/2019.

**CONCLUSION**

65. I submit that this affidavit supports probable cause for a search warrant authorizing the search of the **TARGET ACCOUNTS** described in Attachment A for information described in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

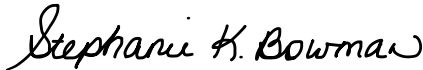
Respectfully submitted,



---

Jonathan P. R. Jones  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on this 25<sup>th</sup> day of January, 2023  
via electronic means, specifically Facetime video.



---

HONORABLE STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF OHIO



**Attachment A**

**Property to Be Searched**

This warrant applies to information associated with the TextNow accounts with username **“mmyumyum11” and “mmyumyum2” (TARGET ACCOUNTS)** that are stored at premises controlled by TextNow Inc., an electronic communications service provider headquarter at 420 Wes Graham Way, 2nd Floor, Waterloo Ontario, N2L 0J6 Canada, but with a United States presence at 1 Sutter Street, Suite 800 San Francisco, CA 94104.

**Attachment B**

**I. Information to be disclosed by TextNow**

To the extent that the information described in Attachment A is within the possession, custody, or control of TextNow, including any messages, records, files, logs, or information that have been deleted but are still available to TextNow, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), TextNow is required to disclose the following information to the government for each account listed in Attachment A:

- a. All contact and personal identifying information for the TextNow accounts with username **“mmyumyum11” and “mmyumyum2” (TARGET ACCOUNTS)** to include but not limited to full name, user identification number, date of birth, gender, contact e-mail, addresses, physical address (including city, state and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- b. All activity logs for the TARGET ACCOUNTS;
- c. All content of text messages sent and received;
- d. All photos and videos uploaded by the TARGET ACCOUNTS and all photos and videos uploaded by any users to the TARGET ACCOUNTS, to include metadata associated with those photos and videos;

e. All records or other information regarding the identification of the devices and internet browsers associated with, or used in connection with, the TARGET ACCOUNT, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

f. All information generated or received by the TARGET ACCOUNTS, including any postings, status updates, comments, networks or groups of which the user is a member, and information about the user's access and use of the TextNow application;

g. All other records and contents of communications and messages made or received by the users, including all public chat messages, private chat messages, group chat messages, chat history, video and voice calling history, and contact lists;

h. All IP logs, including all records of the IP addresses that logged into the TARGET ACCOUNTS;

i. All records of searches performed by the TARGET ACCOUNTS;

j. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

k. All records pertaining to communications between the TARGET ACCOUNTS and any other person regarding the ability to use and access TextNow, including contacts with TextNow support services and records of actions taken

- l. Any original metadata or file information still maintained by TextNow associated with media content sent to or from the user's TextNow account;
- m. Any cookies, web beacons, advertising IDs, and push tokens, associated with the TARGET ACCOUNTS; and
- n. The data listed above in paragraphs A through M shall be produced by TextNow regardless of where it may be stored.

**II. Information to be seized by the government**

- a. All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2422, including the following: All files, documents, communications, images, videos, contacts, metadata, and logs associated with the TARGET ACCOUNTS related to violation of Title 18 U.S.C. Section 2252 and Title 18 U.S.C. Section 2422, along with any evidence that would tend to show the true identities of the persons committing these offenses.
- b. All activity logs and IP logs, including all records of the IP addresses that logged into the account;
- c. Any communications in any format with Minor Victim A or relatives or friends of Minor Victim A;
- d. All account information, including:

- e. All registration, identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- f. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
- g. All privacy settings and other account settings;
- h. All registered devices and accompanying serial numbers and other identifying numbers to include dates of activation, registration, deactivation;
- i. All records pertaining to communications between TextNow and any person regarding the user or the user's TextNow account, including contacts with support services and records of actions taken;
- j. All records that may identify co-conspirators, aiders, abettors, or any other individuals involved in the crime under investigation, including records that may help reveal their true identity and whereabouts; and
- k. All records that may identify any victims of the crime under investigation;